UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,227	09/27/2001	Jeffrey Scott Bardsley	RSW920010166US1	5924

26502 7590 11/04/2004

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 11/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,227	BARDSLEY ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09/27/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 09/27/2001.

DETAILED ACTION

1. Claims 1-12 have been examined.

Title

2. The title of the invention is acceptable.

Priority

3. No claim for priority has been made for this application.

4. The effective filing date for the subject matter defined in the pending claims in this application is 09/27/2001.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 09/27/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

6. The drawings filed on 09/27/2001 are acceptable for examination proceedings.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

8. Claims 1-2, 5, and 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freivald et al. (US Patent Number 6,012,087) hereinafter referred to as Freivald, and further in view of Shanklin et al. (US Patent Number 6,487,666) hereinafter referred to as Shanklin, as evidenced by Chari et al. (US Patent Number 6,425,006) hereinafter referred to as Chari.

9. Regarding claims 1 and 8, Freivald disclosed a system, method, and computer program product for determining a present alert generation rate (See Freivald Col. 13 Lines 11-15), comparing the present alert generation rate with an alert generation rate threshold (See Freivald Col. 13 Lines 15-16), and altering an element of a signature set (See Freivald Col. 13 Lines 35-37) responsive to an outcome of the step of comparing (See Freivald Col. 13 Lines 29-37) (Also see Figure 14). However, Freivald failed to disclose using the alert squelching system and method in an intrusion detection system.

Shanklin teaches a network intrusion detection system in which events are detected based on the signatures of the events (See Shanklin Abstract) and alerts are sent to the system manager (See Shanklin Col. 3 Lines 13-16), but Shanklin failed to disclose squelching the alerts once a certain alert generation threshold was reached.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the network intrusion detection system of Shanklin in the alert squelching system of Freivald, by utilizing the squelching system to lower the alert generation rate of the intrusion detection system.

This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that the system manager of an intrusion detection

system was not overwhelmed by alerts, as well as ensuring that the network was not bottlenecked with alerts.

Furthermore, it is evidenced by Chari that by sending and receiving all alerts, network traffic increases and available bandwidth decreases. Also, the volume of alerts received by the network administrator can overwhelm the administrator (See Chari Col. 2 Lines 55-65).

10. Claims 2 and 9 are rejected for the same reasons as claims 1 and 8 above, and further because Freivald disclosed altering an element of a signature set in order to decrease the alert generation rate (See Freivald Col. 13 Lines 35-45).

11. Regarding claims 5 and 10, the combination of Freivald and Shanklin disclosed monitoring for the occurrence of a signature event (See Shanklin Col. 1 Lines 29-32), counting the number of signature events and comparing it with a threshold (See Shanklin Col. 6 Lines 15-18), and when the count exceeds the threshold generating an alarm (See Shanklin Col. 6 Line 18), recording the time of the alarm in a log (See Freivald Col. 3 Lines 18-20, and Col. 7 Lines 39-41), using the log to determine the alert generation rate (See Freivald Col. 13 Lines 11-15), comparing the alert generation rate with a threshold (See Freivald Col. 13 Lines 15-16), and when the threshold is exceeded, altering an element of the signature set to decrease the alert generation rate (See Freivald Col. 13 Lines 21-29, and 35-45).

12. Claims 3, 6, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Freivald and Shanklin as applied to claims 2, 5, and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

Freivald and Shanklin disclosed altering the signature set in order to reduce the frequency of alert generation by halting the signature detection altogether (See Freivald Col. 13 Lines 35-45), but failed to disclose altering the threshold quantity in order to do so.

Lunt teaches that alarms do not always pertain to individual events, and because they can come very quickly, after the first alarm is generated, subsequent alarms should be suppressed until a second threshold, greater than the first, is reached (See Lunt Page 14 Lines 11-17).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lunt in the alert generation system of Freivald and Shanklin, by suppressing alerts after a first alert, until a higher threshold is reached. This would have been obvious because the ordinary person skilled in the art would have recognized that multiple attacks can occur at the same time and would not want to ignore attacks after the first initial attack.

13. Claims 4, 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Freivald and Shanklin as applied to claims 2, 5, and 10 above respectively, and further in view of Martin et al. (US Patent Number 6,772,349) hereinafter referred to as Martin.

Freivald and Shanklin disclosed altering the signature set in order to reduce the frequency of alert generation by halting the signature detection altogether (See Freivald Col. 13 Lines 35-45), but failed to disclose altering the threshold interval in order to do so.

Martin teaches that in a network intrusion detection system, the time interval used to collect signature data is indirectly proportional to the number of false alarms detected (See Martin Col. 5 Lines 30-38).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Martin in the alert suppressing system of Freivald and Shanklin, by decreasing the time interval once the threshold was broken. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that legitimate alerts were detected while false alarms were reduced.

Conclusion

14. Claims 1-12 have been rejected.

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Vaidya (US Patent Number 6,279,113) disclosed a network intrusion detection system which relied on signatures, in which a log was kept of all detected events matching a signature and the log was used to determine a signature event rate, which was used to determine if an alarm should be generated or not.

16. Please direct all inquiries concerning this communication to Matthew Henning whose telephone number is (571) 272-3790. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Matthew Henning
Assistant Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100